ICRMAT 2020 Proceedings of the International Conference on Research in Management & Technovation pp. 73–78
DOI: 10.15439/2020KM7
ISSN 2300-5963 ACSIS, Vol. 24

Election Infrastructure Security: Grants and Reimbursement to the States for Usage of their National Guards in State Active Duty Status to Provide Cybersecurity for Federal Elections

S. Raschid Muller, Ph.D., MBA
Assistant Professor of Cybersecurity
Capitol Technology University
Laurel, MD, USA
Email - srmuller@captechu.edu
https://orcid.org/0000-0002-1742-7575

Corey E. Thomas, LTC, US Army
Administrative Law Attorney
National Guard Bureau
Washington, DC, USA
Email - cethomas1091@gmail.com

***Abstract*—Because presidential and congressional elections (hereinafter Federal elections) are State-administered activities with a Federal nexus, the Federal government should both reimburse and provide grants to the States when using their National Guards in their State Active Duty (SAD) status[1] to perform cybersecurity assessments and testing before the election, provide general cybersecurity and immediate cyber support in response to a cyber-attack (if required) on Election Day, and provide any post-election support as necessary and appropriate. First, decision-makers must develop an election infrastructure protection plan that effectively utilizes the best assets in a whole-of-nation approach to help meet the three policy goals of election cybersecurity, "access, integrity, and security." Currently, there are gaps in election security that the National Guard is well-position and best-qualified to fill. Once the decision-makers agree on the approach, they can move on to the second step, which is to address how to best support the States in funding the activities through grants, reimbursement, or a combination of the two. This paper explains how the U.S. Constitution, along with specific Federal laws, support the thesis and proposes new legislation that Congress should pass to eliminate current confusion while promoting the unity of effort amongst all stakeholders.**

***Index Terms*—election infrastructure, cybersecurity, National Guard, State Active Duty**

[1] For the purposes of this paper, the term "status" for the National Guard is to mean how the members are commanded, controlled, and financed while serving. When members of the National Guard are placed in their State Active Duty (SAD) status, the Governor of the State has command and control, and their service is financed by their State. When serving in their status under Title 32 of the United States Code (T-32), the Governor of the State has command and control, but their service is financed by the Federal government. When serving in their status under Title 10 of the United States Code (T-10), the President of the United States has command and control, and their service is financed by the Federal government.

I. INTRODUCTION

TO UNDERSTAND how the States administer Federal elections in this country, one must first refer to Article I, § 4 [1], and Article II [23] of the United States (U.S.) Constitution. Article I, § 4 governs congressional elections. While the States set policy regarding the time, place, and manner of congressional elections, Congress may modify the States' policies except for choosing Senators [1]. Under Article II, § 1, while the States still have the responsibility of administering presidential elections, Congress sets the time and date. Thus, the U.S. Constitution clarifies that, while the States administer Federal elections, the Federal government has a direct interest in the process. Additionally, while the Framers did not contemplate electronic elections and cyber-attacks when they drafted the U.S. Constitution in 1787, the powers reserved to the States remain unchanged even though conflicting interpretations often test their permanence. These conflicts arise despite existing laws and policies. As this paper will demonstrate, sometimes the laws and policies provided are not enough to prevent friction between Federal departments/agencies and State governments. National Guard involvement in the provision of cybersecurity for Federal elections is one area where a lack of clarity now exists and must be provided by Congress to ensure the integrity of the election infrastructure now and in the future.

According to Volume 1 of the publicly published and redacted report from the Senate Committee on Intelligence (SCI) [4], during the presidential election of 2016, the U.S. election infrastructure,[2] voting systems, and polling places throughout the States were the focus of multiple cyber-attacks by Russian actors. Thus, the 2016 presidential election made it abundantly clear that the U.S. election system is not safe from cyber-attack. In Volume 3 of the SCI report [17], the Federal government expressed a united interest in

[2] The Secretary of the Department of Homeland Security (DHS) designated election systems a critical infrastructure (CI) in 2017 (DHS, n.d.). Election systems were made a subsector to the Government Facilities CI Sector (DHS, n.d.).

protecting the integrity of U.S. elections by using a whole-of-nation approach [2] to deploy effective cybersecurity measures in protection the election infrastructure [4]. The Fiscal Year 2020 (FY20) National Defense Authorization Act (NDAA) serves as additional evidence of the Federal government's interest in exercising the whole-of-nation strategy to secure the election infrastructure, which includes the provision of funding [9].

Once decision-makers agree upon the general plan and methodology, the focus should turn to the employment of the right Federal, State, and private sector assets. Because election administration is primarily a responsibility of the States [6], foreign actors' election infrastructure cyber-attacks do not immediately constitute homeland defense issues.[3] Unless otherwise determined by the Secretary of Defense (SecDef) or the President of the United States (POTUS), cyber-attacks on the election infrastructure are the first issues of homeland security [22]. As a result, the States and local governments should act as first-responders to the cyber-attack before directly requesting support from the Cybersecurity and Infrastructure Security Agency (CISA).

Historically, the National Guard has served as the first military responder in the homeland [12]. When it comes to the provision of cybersecurity as part of election administration within the States, utilizing the experience and expertise of the State's National Guard should be no different. Utilization of the National Guard must be not only factored into the consolidated election infrastructure security plan and approach, but the Federal government's potential percentage share of any costs incurred should be agreed upon ahead of time. Provision of Federal grants and reimbursement funding for the National Guard to perform cybersecurity functions during Federal elections should not be a point of conflict. Suppose the Federal government can reimburse the States for using their National Guards in their State Active Duty (SAD) status to protect a citizen's right to receive an equal education [14] or respond immediately to a request for assistance during a major disaster or emergency. In that case, it stands to reason that the Federal government can reimburse the States for using their National Guards in their SAD status to protect U.S. citizens' right to vote free from undue influence or coercion. The same holds for the provision of grants.

Many credible studies have addressed the National Guard's usage to protect certain the Federally protected rights of U.S. citizens. Also, Chief, National Guard Bureau Instruction (CNGBI) 3000.04 outlines how the National Guard may provide this civil support in their various statuses. In comparison, the development of specific laws and policies governing how stakeholders should work together in response to a cyber-attack on the election infrastructure is relatively new. Further, there are no studies that address and articulate the thesis of this paper, which is, because Federal elections are State-administered activities with a Federal nexus [9], the Federal government should provide grants and reimbursement funding to the States when using their National Guards in State Active Duty (SAD) status to perform cybersecurity assessments and testing using their Cyber Protection Teams (CPTs)[4] before the election, provide general cybersecurity or immediate cyber support using their Defensive Cyberspace Operations Elements (DCO-Es)[5] in response to a cyber-attack on Election Day or perform any post-election cybersecurity-related activities.

II. The Foundation

A. Reserved under the U.S. Constitution

To understand powers reserved to the States under the U.S. Constitution, one should review Article I, § 8, Clause 16 [22], and the Bill of Rights [1]. While the Congress has the power to place any State National Guard on Federal orders in the service of the United States [21], the appointment of officers and training of the National Guard is reserved to the States [22]. Under the Second Amendment of the U.S. Constitution, the right to maintain a militia is reserved to the States [1]. Today, the State militia is formally referred to as the National Guard. When States utilize their National Guards, they often serve in their SAD status. In some instances, the National Guard's service inures to the benefit of the Federal government. In such cases, the State may seek reimbursement. Thus, when considering whether the Federal government should agree to provide grants or refund funding to the States for cybersecurity activities performed by their National Guards in SAD status during Federal elections, the decision-makers should ask one main question. Did the activities performed by the National Guard in their SAD status serve to the benefit and interest of the Federal government? If so, then it is reasonable to posit that the Federal government should share in the States' costs.

1) Statutory Authority

Current Federal law supports appropriated funds, including homeland security grants, to the States when they perform activities that directly address critical infrastructure threats. For instance, under 6 U.S.C. § 608 [18], Congress authorized federal funding, by way of grants, to States and high-risk urban areas that help enable them to address multi-

[3] When issues of homeland defense arise, even if the issue is a cyber-attack, the Department of Defense (DoD) is the lead federal agency (LFA). In such cases, the status of the National Guard is not in question because when the National Guard is in the service of the United States to augment the DoD, members of the National Guard serve under Title 10 of the United States Code, versus Title 32. In contrast, the DoD is not the LFA in issues of homeland security. The LFA for homeland security is the Department of Homeland Security (DHS).

[4] The mission of a Cyber Protection Team (CPT) is to provide mission assurance and threat mitigation support to United States (U.S.) Critical Infrastructure Key Resources (CIKR) and U.S. Military Services and Combatant Commands key terrain. National Guard personnel on CPTs may serve in their Title 10, Title 32, and State Active Duty statuses (*see* for example https://co.ng.mil/Army/Cyber/).

[5] A Defensive Cyberspace Operations Element (DCO-E) is a State asset serving as a first responder for State Governors and Adjutants General during cyber emergencies (Defensive Cyberspace Operations - Internal Defensive Measures). National Guard personnel on DCO-Es may serve in their Title 32 and State Active Duty (SAD) statuses (*see* for example https://co.ng.mil/Army/Cyber/).

ple threats to critical infrastructure, to include cyber-threats. Under 6 U.S.C. § 660 [19], Congress directed the Director of CISA to, among other things, work with State and local governments, and other entities, to develop a cyber-incident response plan (CIRP) that addresses explicitly cybersecurity risks in all critical infrastructure, which includes the election infrastructure. The National Cyber-Incident Response Plan (NCIRP) [4] was published by DHS in 2016, before the creation of the CISA in 2018. To date, DHS has not updated the plan. Additionally, the plan does not address funding (State reimbursement) or the National Guard in their SAD status when responding to cyber-incidents during Federal elections [4].

To add, the provision of cybersecurity across the United States to multiple entities takes qualified personnel and funding. Even though election security is one of the CISA's top priorities, in November of 2019, the agency reported that it had only 24 cybersecurity advisors and 100 protective advisors to support cyber and physical security assessments of the 16 critical infrastructure sectors [7]. As Figure 1 [3] below demonstrates, CISA personnel provide scanning, assessment, and system testing services to the States and local election jurisdictions. However, the CISA does not have enough personnel to cover the demand, nor does it have a current plan to address cyber-incident response [7]. The National Guard is best-qualified and well-positioned to fill this critical gap for the Federal government.

Service	States	Local election jurisdictions
Continuous scanning of internet-accessible systems for known vulnerabilities	40	161
Assessments of potential network security vulnerabilities	26	20
Remote testing of externally accessible systems for potential vulnerabilities	4	44
Assessments of states' and local jurisdictions' susceptibility to malicious emails	10	5
Educational posters on cybersecurity	19	1,202

Fig. 1 Number of selected Cybersecurity and Infrastructure Security Agency (CISA) services provided to States and local jurisdictions in 2018 & 2019, as of November 6, 2019. Retrieved from, *Election Security: Department of Homeland Security (DHS) Plans are Urgently Needed to Address Identified Challenges Before the 2020 Elections*, February 2020, GAO-20-267, p. 19.

Further, under 52 U.S.C. §§ 20901-21145, also known as the Help American Vote Act (HAVA) of 2002 [10], Congress directed the States to perform multiple acts to include replacement of punch card and lever voting machines, and overall improvement of election administration by developing uniform, non-discriminatory election technology. Implementation of the HAVA requirements gave rise to many physical and cybersecurity threats to the election infrastructure. As Figure 2 above demonstrates, multiple threats exist to the election infrastructure pre-election, Election Day, and post-election. Through its CPTs and DCO-Es, the National

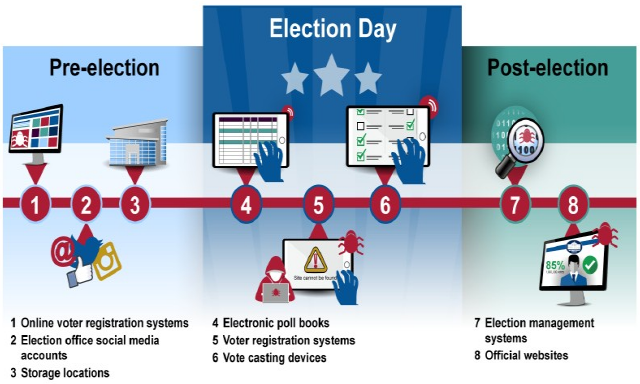

Fig. 2 Threats that exist to the election assets during the three phases of Federal elections. Retrieved from, *Election Security: Department of Homeland Security (DHS) Plans are Urgently Needed to Address Identified Challenges Before the 2020 Elections*, February 2020, GAO-20-267, p. 10.

Guard is well positioned and qualified to provide cybersecurity in each of these phases.

III. State Usage Of Federal Funds To Address Cyber-Threat

Congress has appropriated millions of dollars for State use in election security. In the FY18 Consolidated Appropriations Act, public law (P.L.) 115-141, Congress appropriated $380 million for State use in the administration of Federal elections, which includes election cybersecurity [8]. In the FY20 Consolidated Appropriates Act of 2020 (P.L. 116-93), Congress appropriated an additional $425 million for the same purpose [9]. To finance the usage/transfer of personnel in support of the changes implemented under the rule, the funding authorized under HAVA 2002 does appear purposed for State National Guard personnel. Congress must pass legislation explicitly addressing this issue. The laws must be clear and unambiguous. Because, as Figure 3 below demonstrates, the cybersecurity threats to the election infrastructure are vast. To address those threats, it will take a straightforward, whole-of-nation approach [2] that includes usage of the National Guard's CPTs and DCO-Es.

IV. Recommendations

A. Modify and Pass Election Security Act

Congress should modify and pass the currently proposed Election Security Act [5]. The language contained in the suggested modification should be fashioned after the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121-5189 [15], expressly granting funds to the States for costs incurred while using their National Guard to perform pre-election, Election Day, and post-election cybersecurity activities (i.e., cyber-attack prevention and election system protection measures). The law should also authorize reimbursement of the State's for costs in-

Adversarial/malicious	
Hackers/hacktivists	Hackers who break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists, or ideologically motivated actors who take advantage of cyber vulnerabilities to further political goals.
Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) whose position within the organization allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. These individuals engage in purely malicious activities and should not be confused with nonmalicious insider accidents.
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs that use cyber tools as part of their information-gathering and espionage activities.
Criminal groups and organized crime	Criminal groups who seek to attack systems for monetary gain. Specifically, organized criminal groups that leverage cyber vulnerabilities to commit identity theft, online fraud, and computer extortion.
Terrorists	Terrorists who seek to destroy, incapacitate, or purposefully misuse critical infrastructures in order to threaten national security, weaken the economy, and damage public morale and confidence.
Unknown malicious outsiders	Threat sources/agents who, due to their success in remaining anonymous, are unable to be classified as one of the five types of threat sources/agents listed above.

Fig. 3 The sources of cybersecurity threats to the election infrastructure. Retrieved from, *Election Security: Department of Homeland Security (DHS) Plans are Urgently Needed to Address Identified Challenges Before the 2020 Elections*, February 2020, GAO-20-267, p. 34.

curred to provide additional National Guard personnel to respond to any cyber-attack on a Federal election (i.e., cyber-incident response). Suppose Congress does not pass the Election Security Act. In that case, the new legislation's language should be nested under Subtitle II, Voting Assistance, and Election Administration of Title 52 of the United States Code, Voting, and Elections [24]. Whether integrated into proposed or current law, the new rule should, among other things, specifically address grants or reimbursement funding for using the Cybersecurity Relief Fund (CRF) and clearly outline the ability of POTUS, acting through the Director of CISA, to authorize the release of those funds. The grant and reimbursement funds represent the Federal government's percentage share of the Federal election administration expenses incurred by the States while providing the necessary cybersecurity not covered by HAVA 2002. With that said, neither the Governors nor POTUS should have to make any declarations similar to those required under the Stafford Act. Why? Because, unlike the impact, or potential impact, of a hurricane, tornado, or earthquake that may be purely a State responsibility, a Federal election by its very nature is a matter of Federal interest that bears Federal responsibility from the onset. Like current grants that States are receiving for election administration improvement, States should receive grants for general cybersecurity activities performed by members of the National Guard in their SAD status pre-election, Election Day, and post-election. In the event of a cyber-attack, the States should be reimbursed for using their National Guard in SAD status for cyber incident response. An example of the section language suggested appears in Appendix 1.

4.2 Create a Federal Policy Governing use of the National Guard for Federal Elections

Second, Congress should draft a law similar to 10 U.S.C. § 275 [11] directing the Secretary of Defense, through the Chief, National Guard Bureau in partnership with the Director of CISA, to prescribe policy that not only aligns with the new law, but also specifically authorizes the use of the National Guard in their SAD status to perform cybersecurity functions during the three phases of the election process, outlines the cyber-incident response process, and describes how States are to be Federally reimbursed for costs incurred. This new law should be nested under Chapter 1011 of Title 10 of the United States Code, National Guard Bureau [13]. An example of the section language suggested for the CAA appears in Appendix 2.

V. Conclusion

In the U.S. Constitution the Framers tasked the States with the responsibility of Federal election administration. This responsibility has not changed since 1787. While it is clear that States bear the responsibility to administer Federal elections [9], the Federal government directly benefits from the work performed. It should, therefore, provide funds to the States in return. To the Federal government's credit, millions of dollars have already been allocated explicitly to the States to support the improvement of election system security. The HAVA of 2002 is one great example. However, one critical gap in funding remains. The funding gap lies in the National Guard conduct of Federal election cybersecurity activities pre-election, Election Day, and post-election. Because the Federal government receives a direct benefit from this Federal election cybersecurity support provided, the Federal government should share the cost by way of grants or reimbursement. Passage of new legislation that addresses explicitly provision of grants or reimbursement funding to the States for using their National Guard in SAD status to perform cybersecurity activities before, during, and after Federal elections will demand a whole-of-nation approach [2] led by the CISA with support from the DoD and the National Guard. Such a collaborative effort will most certainly help the Federal government draw closer to the three policy goals of election cybersecurity; "access, integrity, and security" [8].

Appendix 1

Sample Draft Language of Proposed Cybersecurity Legislation (Stafford Act, 1988, §§ 101, 202)

"[§0123]. Congressional findings and declarations

(a) The Congress hereby finds and declares that-

(1) because [any cyber-attack conducted during a congressional or presidential election (Federal election) is a direct attack on the election infrastructure of the United States]; and

(2) because [cyber-attacks conducted during a Federal election can] disrupt the normal functioning of [the Federal

government, and adversely affect public trust and confidence in the electoral process]; special measures, designed to assist the efforts of the affected States (. . .) in [providing cybersecurity during a Federal election], are necessary.

(b) It is the intent of the Congress, by this chapter, to provide an orderly and continuing means of assistance by the Federal Government to [the States] (. . .) in carrying out their responsibilities to [administer Federal elections] by-

(1) revising and broadening the scope of existing [election security] programs;

(2) encouraging the development of comprehensive [cyber-attack preparedness, response, and recovery] assistance plans, programs, capabilities, and organizations by the States (. . .);

(3) achieving greater coordination and responsiveness of [cyber-attack] preparedness, [response] and relief programs;

(4) encouraging individuals and [States] (. . .) to protect themselves [from cyber-attack] to [help] supplement or replace governmental assistance;

(5) encouraging [cyber-attack] mitigation, [response, and recovery] measures to reduce losses from [cyber-attacks], including development of [cyber-attack mitigation, response, and recovery] regulations; and

(6) providing Federal assistance programs for both public and private losses sustained during [Federal elections as a result of a cyber-attack].

[§0456. Federal Election Cybersecurity]
(. . .)

(a) Establishment of Program – [In addition to those funds authorized for distribution under the Help America Vote Act], the President may establish a program to provide (. . .) financial assistance to States (. . .) to assist in the implementation of [election cybersecurity activities to mitigate the risk of potential cyber-attacks, as well as respond to and recover from cyber-attacks]. [These measures shall be] cost-effective and (. . .) designed to reduce (. . .) damage and destruction of property, including damage to [the election infrastructure].

(b) Approval by President - If the President determines that a State (. . .) has identified [Federal election cyber-threats] in areas under its jurisdiction and has demonstrated the ability to form effective public-private [cybersecurity risk] mitigation partnerships, the President, using amounts in the [Cybersecurity Relief Fund (CRF)] (. . .) may provide financial assistance to the State (. . .) to be used in accordance with subsection (c) of this section.

(c) Uses of (. . .) Financial Assistance –

(1) In General - Financial assistance provided under this section—

(A) shall be used by States principally to implement [cyber-attack mitigation, response, and recovery] measures [during Federal elections] that are cost-effective and are described in proposals approved by the President under this section; and

(B) may be used -

(i) to support effective public-private [cybersecurity] partnerships;

(ii) to improve the assessment of a [State's election infrastructure] vulnerability to [cyber-attack]; or

(iii) to establish [cyber-attack] mitigation, [response, and recovery] priorities, and an appropriate [cyber-attack] mitigation, [response, and recovery] plan for the [State during Federal elections. This plan may include funding of the State's National Guard in their State Active Duty status].

(d) Cost Sharing.

(1) [Once approved by the President], financial assistance provided under this section may contribute up to 75 percent of the total cost of [cybersecurity activities performed by a State prior to, during, and after a Federal election. The President may accept this general rule and approve the Federal government to contribute up to 100 percent of the total cost of cybersecurity activities performed by a State prior to, during, and after a Federal election].

(2) the non-Federal share shall be paid from funds made available by the State."

APPENDIX 2

Sample Draft Legislation Directing Promulgation of Federal Policy for Use of the National Guard to Provide Cybersecurity During Federal Elections

(Restriction on Direct Participation by Military Personnel, 2016, § 275)

"[§0123 Use of the National Guard for Cybersecurity During Federal Elections]

[The Chief, National Guard Bureau, with the concurrence of the Secretary of Defense, and advice of the Director, Cybersecurity, Infrastructure Security Agency], shall prescribe regulations as may be necessary to ensure that [any Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM)] conducted under this chapter [aligns with the Federal Election Cybersecurity Assistance Act (FECAA) and, unless otherwise authorized by law, does not constitute Offensive Cyberspace Operations (OCO) or DCO-Response Actions (DCO-RA). Such policy shall specifically address State usage, State funding, Federal funding, and Federal reimbursement, of their National Guard to perform cybersecurity activities prior to, during, and after Federal elections in the following statuses: State Active Duty (SAD), 32 U.S.C. § 502(a), 32 U.S.C. § 502(f)(1), and 32 U.S.C. § 502(f)(2)] (. . .)."

APPENDIX 3

Figures

Figure 1. A graphic depicting the number of selected Cybersecurity and Infrastructure Security Agency (CISA) services provided to States and local jurisdictions in 2018 AND 2019, as of November 6, 2019. Retrieved from https://www.gao.gov/assets/710/704314.pdf

Figure 2. A graphic depicting the threats that exist to the election assets during the three phases of Federal elections. Retrieved from https://www.gao.gov/assets/710/704314.pdf

Figure 3. A graphic depicting the sources of cybersecurity threats to the election infrastructure. https://www.gao.-gov/assets/710/704314.pdf

REFERENCES

[1] Bill of Rights, U.S. Constitution, Amendments I-X, March 4, 1789.

[2] Cybersecurity and Information Security Agency (DISA), Protect2020 Strategic Plan, February 2020. https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan_FINAL%202.7.20%20508.pdf [Accessed September 9, 2020]

[3] Department of Homeland Security (DHS), DHS cybersecurity services catalog for election infrastructure, July 2017. https://www.eac.gov/sites/default/files/eac_assets/1/6/DHS_Cybersecurity_Services_Catalog_fo _Election_Infrastructure.pdf [Accessed September 9, 2020]

[4] Department of Homeland Security (DHS), National Cyber Incident Response Plan (NCIRP), December 2016. https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf [Accessed September 9, 2020]

[5] Election Security Act S. 1540, 116th Congress U.S. Congress, May 16, 2019. https://www.congress.gov/116/bills/s1540/BILLS-116s1540is.pdf [Accessed September 3, 2020]

[6] Government Accountability Office (GAO) Report # 05-956, Federal efforts to improve security and reliability of electronic voting systems are underway, but key activities need to be completed, September 2005. https://www.gao.gov/assets/250/247851.pdf [Accessed September 3, 2020]

[7] Government Accountability Office (GAO) Report # 20-267, Election security: DHS plans are urgently needed to address identified challenges before the 2020 elections, February 2020. https://www.gao.gov/assets/710/704314.pdf [Accessed September 3, 2020]

[8] R. Garrett, "Campaign and election security policy: brief introduction", Congressional Research Service, July 9, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11265 [Accessed September 1, 2020]

[9] R. Garrett, K. Shanton, and S. Eckman, "Campaign and election security policy: overview and recent developments", Congressional Research Service, January 2, 2020. https://crsreports.congress.gov/product/pdf/R/R46146 [Accessed September 1, 2020]

[10] Help America Vote Act (HAVA), P.L. 107-252, 52 U.S.C. §§ 20901-21145, October 29, 2002. https://www.congress.gov/107/plaws/publ252/PLAW-107publ252.pdf [Accessed September 5, 2020]

[11] Military Support for Civilian Law Enforcement Agencies, Restriction on Direct Participation by Military Personnel, 10 U.S.C. § 275, 2016. https://uscode.house.gov/view.xhtml?edition=prelim&req=granuleid%3AUSC-prelim-title10-section275&num=0&hl=false [Accessed September 5, 2020]

[12] National Guard Bureau (NGB), 2020 National Guard posture statement: Implementing the national defense strategy, 2020. https://www.nationalguard.mil/portals/31/Documents/PostureStatements/2020-National-Guard-Bureau-Posture-Statement.pdf [Accessed September 6, 2020]

[13] National Guard Bureau, 10 U.S.C. §§ 10501-10508, 2020. https://www.law.cornell.edu/uscode/text/10/10508 [Accessed September 6, 2020]

[14] National Guard Regulation (NGR) 500-5, National Guard Domestic Law Enforcement Support and Mission Assurance Operations. Funding, August 18, 2010. https://www.ngbpmc.ng.mil/Portals/27/Publications/ngr/ngr%20500-5.pdf?ver=2018-09-07-082540-767 [Accessed September 5, 2020]

[15] Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), P.L. 93-288, 42 U.S.C. §§ 5121-5189, November 23, 1988. https://www.fema.gov/sites/default/files/2020-03/stafford-act_2019.pdf [Accessed September 5, 2020]

[16] Senate Committee on Intelligence (SCI), "Russian active measures, campaigns, and interference in the 2016 U.S. election", Volume 1 – Russian efforts against election infrastructure with additional views. United States Senate (redacted), n.d. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [Accessed September 5, 2020]

[17] Senate Committee on Intelligence (SCI), "Russian active measures, campaigns, and interference in the 2016 U.S. election", Volume 3 – U.S. government response to Russian activities. United States Senate (redacted), n.d. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf [Accessed September 5, 2020]

[18] U.S.C. § 608, Domestic Security, Prioritization, 6, 2001. https://www.govinfo.gov/app/details/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapXV-partA-sec608 [Accessed September 15, 2020]

[19] U.S.C. § 660, Domestic Security, Cybersecurity Plans, 6, 2018. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section660&num=0&edition=prelim [Accessed September 15, 2020]

[20] U.S.C. Art. I, § 4., U.S. Constitution, 1787. https://www.law.cornell.edu/constitution/articlei [Accessed September 15, 2020]

[21] U.S.C. Art. I, § 8, cl. 15., U.S. Constitution, 1787. https://www.law.cornell.edu/constitution/articlei [Accessed September 15, 2020]

[22] U.S.C. Art. I, § 8, cl. 16., U.S. Constitution, 1787. https://www.law.cornell.edu/constitution/articlei [Accessed September 15, 2020]

[23] U.S.C., Art. II, U.S. Constitution, 1787. https://www.law.cornell.edu/constitution/articleii [Accessed September 15, 2020]

[24] Voting Assistance and Election Administration, 52 U.S.C. §§ 20101-21145, September 28, 1984. https://www.law.cornell.edu/uscode/text/52/subtitle-II [Accessed September 15, 2020]

Dr. S. Raschid Muller is a Senior Cybersecurity SME with the Department of Defense (DoD) at Fort Meade, Maryland. He teaches Cybersecurity at the undergraduate and graduate levels at Arizona State University, University of Maryland Global Campus, and Capitol Technology University. Dr. Muller is a 2020 Brookings Institute Fellow (LEGIS) currently serving on the House Committee for Homeland Security assigned to the Cybersecurity, Infrastructure Protection, and Innovation subcommittee in the United States Congress. He will attend U.C. Berkeley's Executive Leadership Academy in 2021 as a Fellow in the Goldman School of Public Policy. He is a member of IEEE, ISACA, NDIA, and AFCEA.

LTC Corey E. Thomas, Esq. is a Senior Administrative Law Attorney in the United States Army Judge Advocate General Corps. He is a graduate of Morehouse College, University of Arkansas-Little Rock Bowen School of Law, The General Staff and Command College, and National Defense University. Before joining the National Guard Bureau, he served as the Director for Domestic Operations at The Center for Law and Military Operations (TJAGLCS) in Charlottesville, Virginia. He is admitted to practice law in Arkansas state courts, the federal Eastern and Western Districts of Arkansas, the United States Court of Appeals for the Armed Forces, and the United States Supreme Court.